



## **Redes e Comunicação de Dados**

### **Relatório Final**

**Curso:** Engenharia de Sistema e Informática



#### **Docente:**

Ibrahino Moreno

#### **Discentes:**

João Cláudio-9529

Emerson Patrik-9596

Bruno Oliveira-9415

## Índice

Introdução .....	1
2 Fundamentacao teorica .....	2
2.1 Historial da Comunicação e Redes e Comunicação de Dados .....	2
2.2 Definição de Redes e Comunicação de Dados .....	3
2.3 Definição de Comunicação.....	4
2.4 Principais equipamentos de interligação .....	4
2.6 Tecnologias de Comunicação .....	7
2.7 Modelos e Protocolos de Comunicação.....	8
Modelo OSI .....	16
2.8 Segurança em Redes de Comunicação .....	18
3. Caso Prático da Empresa/Organização .....	20
3.1 Caracterização da entidade em estudo .....	20
3.2 Análise da situação atual .....	21
3.2.1 Projeto Lógico.....	22
3.2.2 Projeto Físico .....	25
3.3 Proposta de melhorias.....	25
Conclusão .....	26
Bibiografia .....	27

## **Introdução**

Hoje, é possível conectar os mais diversos dispositivos para que eles conversem entre si, troquem informações e funcionem de forma segura e integrada

Na actualidade vivemos na chamada Sociedade da Informação onde é fundamental estar informado e comunicar por telefone ou através da Internet e telemóvel. As novas tecnologias TIC têm uma grande importância na vida das pessoas, invadindo todas as áreas do quotidiano, incluindo a Educação, a área profissional e do lazer.

Este trabalho foi desenvolvido no sentido de que as novas tecnologias sejam vistas como mais uma ferramenta de auxílio ao processo de educação, negócio, como dinamizadora do processo de ensino e como instigadoras para a melhoria da aprendizagem, eficácia no sector empresarial portanto este trabalho visa mostrar o que tínhamos apreendido durante as aulas de rede de comunicação e correlacionar com a prática feita na empresa que no nosso caso é a empresa Power Solution, onde fizemos questionário sobre equipamento da rede existente nesta empresa.

## **2 Fundamentacao teorica**

### **2.1 Historial da Comunicação e Redes e Comunicação de Dados**

Tudo começou por volta de 1960, quando a comunicação se dava pela rede telefônica. Nesse período, foram desenvolvidos micro e minicomputadores de bom desempenho. Mas faltava um meio para unir essas máquinas e crescia a necessidade de compartilhar informações entre usuários de diferentes regiões.

Vários pesquisadores iniciaram seus estudos nesse época no MIT, no Rand Institute e no National Physical Laboratory. A união dos três trabalhos fez surgir o projeto ARPA (Agência de Projetos de Pesquisa Avançada), que deu origem à ARPAnet, precursora da grande rede mundial, a internet, foi a primeira rede de computadores do mundo.

Os primeiros computadores foram chamados de IMPs (interface message processors). No mesmo ano em que o homem pisou na lua, em 1969, foi instalado o primeiro IMP na Universidade da Califórnia, com três IMPs adicionais.

Em 1970, começaram a surgir novas redes de computação de pacotes, como a ALOHAnet, rede de microondas por rádio que interligava as ilhas do Havaí, e a TELENET, rede de interligação de pacotes comerciais baseada na tecnologia da ARPAnet.

O número de pequenas redes foi crescendo tanto que Robert Metcalfe apresentou os princípios de uma rede local, a ETHERNET, que depois deram origem a LANs de curta distância, com supervisão da DARPA (Agência de Projetos de Pesquisa Avançada de Defesa).

Nesse período, também foi criado o protocolo TCP (transmission control protocol), responsável por enviar os pacotes em sequência e de forma confiável. Com o tempo, o serviço foi sendo modificado e o TCP ficou responsável por organizar a chegada dos pacotes, enquanto o IP tem a função de envio e o UDP controla o fluxo de voz.

No final daquela década, cerca de 200 computadores já estavam conectados à ARPAnet, principalmente porque ela foi usada para a comunicação entre os militares durante a Guerra Fria. Terminada essa época, a ARPAnet deixou de ser interessante para eles e foi transferida para as universidades.

Foi quando os pesquisadores começaram a transmitir essa comunicação para outras nações, chegando a ter 100 mil máquinas na rede ao final da década de 1980. Assim se formou uma grande rede mundial, que começou a ser chamada de internet. Depois disso, em 1983, o protocolo TCP/IP se tornou oficial e passou a ser obrigatório em todos os computadores.

Foi também nessa época que surgiu o NSFNET, o backbone primário que fornecia acesso aos outros centros de computação, e o DNS (Domain Name System), que permitia transformar endereços em palavras e letras, que são mais fáceis de memorizar.

## 2.2 Definição de Redes e Comunicação de Dados

Na informática e na telecomunicação a rede é um conjunto de dois ou mais dispositivos eletrônicos de computação interligados por um sistema de comunicação digital, guiados por um conjunto de regras para compartilhar entre si informação, serviços e, recursos físicos e lógicos.

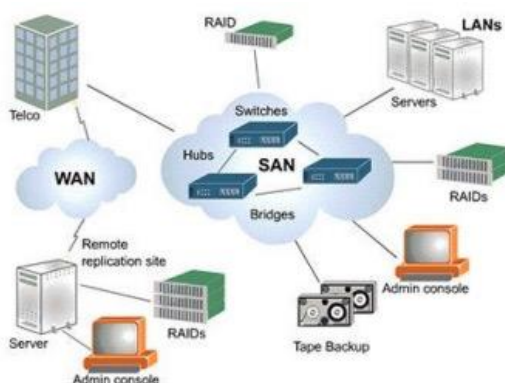


Figura 1: Exemplo de um tipo de Rede

A **Comunicação Dados** é uma disciplina da área de “Ciências da Computação” que trata da transmissão de informação entre sistemas computacionais e dispositivos diferentes através de um meio de transmissão. A transmissão de informação pressupõe a passagem de sinais através dos meios físicos de comunicação que compõem as redes.

### 2.3 Definição de Comunicação

A comunicação é um processo que envolve a troca de informações entre dois ou mais interlocutores por meio de signos e regras semióticas mutuamente entendíveis. Trata-se de um processo social primário, que permite criar e interpretar mensagens que provocam uma resposta.

### 2.4 Principais equipamentos de interligação

- **Equipamentos passivos:** cabos, conectores, distribuidores, ...
- **Equipamentos informáticos:** PC's e servidores
- **Equipamentos activos:** repetidores, hubs, switches, routers

Permitem:

- A ligação de sistemas terminais à rede
- A interligação de vários troços ou segmentos dentro de uma rede
- A interligação de redes distintas

**Repetidores** são dispositivos de hardware utilizados para conexão de dois ou mais segmentos de uma rede local.



*Figura 2. Repetidor*

**Hub** é um repetidor que promove um ponto de conexão física entre os equipamentos de uma rede e são utilizados para ligar os equipamentos que compõem a rede LAN.



*Figura 3: Hub*

**Switch** é um dispositivo com várias entradas que permitem a interligação ao posto de trabalho, servidores e a outros equipamentos numa topologia física em estrela.



*Figura 4: Switch*

Router é um equipamento usado para fazer comutação de protocolos, a comunicação entre diferentes redes de computadores e provedor de serviço de internet assim conseguindo a comunicação distante entre si.



*Figura 5: Router*

Distribuidores que podem ser também designado de bastidores ou armários repetidores, é um armário que têm por norma todo o material associado à rede local do edifício e ainda o equipamento destinado às comunicações com o exterior.



*Figura 6: Bastidores*

Os **cabos** de rede são hardware de rede usado para conectar um dispositivo de rede a outros dispositivos de rede ou para conectar dois ou mais computadores para compartilhar impressoras, scanners etc.



*Figura 7: Cabo*

**Computador** é um conjunto de componentes eletrônicos capaz de variados tipos de tratamento automático de informações ou seja é uma máquina que processa informações eletronicamente,



na forma de dados e pode ser programado para as mais diversas tarefas.



*Figura 8: Computador*

## **2.6 Tecnologias de Comunicação**

A Tecnologia de Comunicação nas empresas tem sido amplamente utilizada por gestores de diferentes áreas a fim de proporcionar uma melhor comunicação entre os colaboradores e até com público.

Os consumidores têm consciência do seu poder de compra, por conta da grande quantidade de informações disponíveis e de fácil acesso. Assim, com a alta concorrência, a demanda pela superioridade nos produtos e serviços, bem como no atendimento ao cliente prestado pelas empresas, está aumentando drasticamente.

Nesse sentido, para ganhar vantagem competitiva e reverter esse cenário, a tecnologia de comunicação está sendo bastante utilizada. Ao utilizar softwares, hardwares e a telecomunicação de forma integrada, ela consegue quebrar barreiras sociais, culturais e até tecnológicas que impedem o sucesso do negócio.

A Tecnologia da Comunicação nada mais é que um conjunto de ferramentas tecnológicas utilizadas de forma incorporada, para que a empresa consiga chegar mais rápido e intuitivamente ao seu objetivo de negócio.

Ao ser implementada, a tecnologia de comunicação consegue automatizar processos, melhorar a aprendizagem, reduzir custos e facilitar pesquisas, sejam elas internas ou externas. Além disso, por tratar os procedimentos com uma comunicação mais eficaz e automatizada, promove a melhoria na experiência do cliente e gera maior satisfação por parte do consumidor em relação à marca.

## **Exemplos de Tecnologia de comunicação**

### **E-mail**

O e-mail ainda é uma ferramenta indispensável nos dias de hoje. Além de poder ser utilizado na comunicação interna de empresas, no marketing e até como canal de atendimento, ele consegue alcançar uma grande quantidade de pessoas e abranger muitas informações.

### **VoIP**

Sem dúvida, o VoIP é a maneira perfeita de otimizar a comunicação de uma forma muito mais barata. Basicamente, trata-se de uma tecnologia que oferece chamadas por meio de alternativas ao telefone, o que reduz o tempo e o trabalho de telefonistas.

## **2.7 Modelos e Protocolos de Comunicação**

Toda comunicação exige um conjunto de regras que devem ser respeitadas pelas duas entidades que se comunicam.

Protocolos de rede são um conjunto de normas que permitem que qualquer máquina conectada à internet possa se comunicar com outra também já conectada na rede.

É assim que qualquer utilizador consegue enviar e receber mensagens instantâneas, baixar e subir arquivos no seu site e acessar qualquer tipo de domínio na web.

Os protocolos de internet funciona dessa forma, como uma espécie de “língua universal” entre computadores. Independente do fabricante e do sistema operacional instalado, essa linguagem é interpretada por todas as máquinas igualmente.

Assim, não é necessário usar qualquer tipo de software extra para que um computador possa entender os protocolos de rede. É desse jeito que ele se comunica com outro computador ligado à rede mundial de computadores sem qualquer problema.

Os tipos de protocolos de rede são divididos de acordo com a sua natureza do serviço disponibilizado. E também em qual camada de profundidade estão localizados na rede de internet.

Essas camadas, junto com alguns exemplos de protocolos, são:

**Camada de Aplicação:** WWW (navegação web), HTTP, SMTP (emails), FTP (transferência de arquivos) e SSH. Usada pelos programas para enviar e receber dados de outros programas pela própria internet.

**Camada de Transporte:** TCP, UDP e SCTP. Para transporte de arquivos recebidos da camada anterior. Aqui acontece a organização e a transformação deles em pacotes menores, que serão enviados à rede.

**Camada de Rede:** IP (IPv4 e IPv6). Os arquivos empacotados na camada anterior são recebidos e anexados ao IP da máquina que envia e que recebe os dados. Daqui, são enviados pela internet usando a próxima camada.

**Camada de Estrutura Física:** Ethernet e Modem. É a camada que executa o recebimento ou envio de arquivos na web.

## **Tipos de Protocolos de Rede**

### **1. Protocolo TCP/IP**

**TCP/IP** é o acrônimo de dois protocolos combinados: o **TCP** (*Transmission Control Protocol*, que significa **Protocolo de Controle de Transmissão**) e **IP** (*Internet Protocol*, que significa **Protocolo de Internet**).

Dentre todos os protocolos de rede, juntos, eles formam a base de envio e recebimento de dados por toda a internet.

O protocolo TCP/IP surgiu em 1969 nos Estados Unidos durante uma série de pesquisas militares da **ARPANET**.

Ele foi criado para permitir a comunicação entre sistemas de computadores de centros de estudos e organizações militares espalhadas em vários pontos do planeta.

A ideia era oferecer uma troca rápida de mensagens entre computadores conectados a uma rede inédita. E, nesse meio termo, identificar as melhores rotas entre dois locais, mas também encontrar rotas alternativas, quando necessárias.

Ou seja, um protocolo que garantisse a conexão mesmo em caso de um cataclisma nuclear.

O protocolo TCP/IP é, na verdade, um conjunto de protocolos que facilitam a comunicação entre duas máquinas conectadas à rede.

## **2. Protocolo HTTP**

**HTTP** é a sigla para *Hypertext Transfer Protocol*, que significa **Protocolo de Transferência de Hipertexto**. Ele é o mais básico e usado para navegação em sites da internet.

O **protocolo HTTP** funciona também como uma conexão entre o cliente e o servidor. Neste caso, o cliente é o navegador que você usa para acessar a internet. E o servidor é aquele em que um site ou domínio está hospedado na rede.

O navegador envia um pedido de acesso a uma página. Essa requisição acontece quando colocamos o endereço de algum site no campo de buscas no navegador. É assim que se acessa qualquer site na rede.

Enquanto isso, o servidor manda uma resposta de permissão de acesso. Com ela, vêm os arquivos que formam a página que o usuário que acessar. Além, também, das informações de hipertexto que fazem outras requisições para levar o leitor a outras páginas através de links.

Se a solicitação vier com algum problema, como o **Erro 500**, o utilizador não consegue acessar o site.

### 3. Protocolo HTTPS

**HTTPS** é a sigla para *Hyper Text Transfer Secure*, que significa **Protocolo de Transferência de Hipertexto Seguro**.

O **protocolo HTTPS** é e funciona de forma exatamente igual ao HTTP. A diferença da letra “S” na sigla é uma camada extra de proteção, indicando que sites e domínios que possuem esse protocolo são seguros para o usuário acessar.

O protocolo HTTPS é muito usado por sites com sistemas de pagamentos que dependem proteção para assegurar dados, informações de conta e cartão de créditos dos utilizador.

Essa proteção é feita por certificação digital, que cria uma criptografia para impedir que ameaças e ataques na internet tenham acesso indevido às informações dos usuários.

O HTTPS aparece em um navegador quando o site acessado possui um **Certificado SSL** instalado. O SSL cria um canal de proteção entre o cliente e o servidor, adicionando a letra “S” ao HTTP e reforçando uma camada extra de segurança.

### 4. Protocolo DHCP

**DHCP** é o acrônimo para *Dynamic Host Configuration Protocol*, que significa, em português adaptado, **Protocolo de Configuração Dinâmica de Endereços de Rede**. Ele permite que os computadores consigam um endereço de IP automaticamente.

Por meio de um servidor, o protocolo DHCP é capaz de obter, sem a necessidade de configuração manual, endereços de IPs para cada um dos computadores (ou dispositivos móveis) ligados a uma rede de internet.

Uma vez que uma máquina obtém um endereço de IP, ele fica indisponível para uso naquele momento. Quando ela é desligada ou desconectada da internet, o endereço de IP, antes volta a ficar disponível para ser usado por qualquer nova máquina ligada na conexão.

O protocolo DHCP funciona de três maneiras diferentes. São elas:

**Automática.** Um IP é definido automaticamente para uma máquina que se conecta na. Neste caso, uma quantidade de IPs é delimitada para ser usada dentro de uma rede de internet. Qualquer computador que se ligar a ela recebe, automaticamente, um, destes IPs definidos.

**Dinâmica.** Como o termo sugere, uma máquina que se conecta à rede de internet recebe um IP dinâmico pelo período em que continuar conectado. Se a máquina for desligada ou se desconectar da rede, ela perde este IP usado e usa um novo assim que a conexão for restabelecida.

**Manual.** O protocolo DHCP define um IP para uma máquina de acordo com o valor de MAC (Medium Access Control) da placa de rede em que ela está conectada. Este IP é único e estático, sendo que este recurso é usado quando é preciso que um computador tenha um IP fixo.

## 5. Protocolo FTP

**FTP** é a sigla para *File Transfer Protocol*, que significa **Protocolo de Transferência de Arquivos**. Ele surgiu antes mesmo do padrão TCP/IP, que é a base das conexões de internet. É o modo mais simples de transferir dados entre duas máquinas pela rede.

O **protocolo FTP** funciona com dois tipos de conexão:

**Cliente.** É o computador que faz o pedido de conexão com o servidor para pegar algum arquivo ou documento dele.

**Servidor.** É o computador que recebe o pedido de conexão com o cliente para fornecer um arquivo ou documento dele.

A conexão do cliente com servidor feita pelo cliente na porta 21 do servidor. Essa conexão fica aberta durante toda a sessão para permitir os comandos necessários, como identificação de contas e senhas.

Na transferência de arquivos, a conexão é ativada pela porta 20 do servidor a alguma porta do cliente previamente estabelecida ou comunicada pelo próprio servidor.

O FTP é muito útil caso o utilizador o perca o acesso ao painel de controle do seu site WordPress, por exemplo. Nesta situação, pode usar uma ferramenta de FTP para ajustar códigos de página, colocar ou apagar arquivos ou resolver qualquer outro problema no seu site.

## 6. Protocolo SFTP

**SFTP** é a sigla para *Simple File Transfer Protocol*, que significa **Protocolo de Transferência Simples de Arquivos**. Ele é, basicamente, o protocolo FTP com uma camada de proteção a mais aos arquivos transferidos.

O que diferencia o **protocolo SFTP** do protocolo FTP é que o primeiro utiliza a tecnologia **SSH** (*Secure Shell*) para autenticar e proteger a conexão entre cliente e servidor.

No protocolo SFTP, a troca de informações não é feita por um canal livre direto, mas por pacotes SSH. Assim, o usuário define a quantidade de arquivos que quer transferir ao mesmo tempo em que cria um sistema de senhas para reforçar a segurança do processo.

## 7. Protocolo SSH

**SSH** é a sigla para *Secure Shell* que, em português adaptado, significa Bloqueio de Segurança. É um dos protocolos específicos de segurança de troca de arquivos entre cliente e servidor.

O **protocolo SSH** funciona a partir de uma chave pública, que verifica e autentica a legitimidade do servidor que o cliente quer acessar (ou vice-versa). Esse acesso é feito por um login e senha, tornando a conexão entre computadores mais protegida.

Com o SSH, o usuário de internet consegue definir um sistema de proteção para seu site sem comprometer o desempenho dele. Ele fortifica a segurança do seu projeto ao mesmo tempo em que trabalha na transferência de arquivos de uma maneira confiável e estável.

## 8. Protocolo POP3

**POP3** é o acrônimo para *Post Office Protocol 3*, que significa, excluindo o número, **Protocolo de Correios**. Ele é usado para mensagens eletrônicas, ou seja, os populares emails.

O **protocolo POP3** funciona como se fosse uma caixa-postal dos Correios. Um servidor de email recebe e armazena diversas mensagens. Então, o cliente se conecta e se autentica ao servidor da caixa de correio para poder acessar e ler essas mensagens lá guardadas.

Com isso, as mensagens armazenadas no servidor são transferidas em sequência para a máquina do cliente. No final, a conexão é terminada e o cliente pode ler suas mensagens até mesmo quando estiver offline. Esta é uma das suas grandes características, inclusive.

## 9. Protocolo SMTP

**SMTP** é a sigla para *Simple Mail Transfer Protocol*, que significa **Protocolo de Transferência de Correio Simples**. Diferente do POP3, o **protocolo SMTP** é voltado para o **envio** de mensagens eletrônicas (emails).



A mensagem sai da máquina do cliente e, depois de ter um ou mais destinatários determinados, é autenticada e enviada para o servidor. Lá, os destinatários recebem as mensagens enviadas para o servidor, que são codificadas e recebidas pelo protocolo POP3.

O protocolo SMTP é eficiente por sua simplicidade, mas também é um pouco limitado. Ele se baseia somente em texto. Ou seja, para envio de arquivos, pastas ou mídias, é preciso extensões que convertem esses arquivos no formato de texto.

## 10. Protocolo IMAP

**IMAP** é o acrônimo para *Internet Message Access Protocol*, que significa **Protocolo de Acesso à Mensagem de Internet**. Assim como os dois anteriores, o protocolo IMAP também é voltado para envio e recebimento de emails.

Mas, diferentemente deles, o protocolo IMAP permite que o usuário acesse e gerencie seus arquivos e mensagens diretamente no próprio servidor. Ou seja, não é preciso esperar que as mensagens enviadas ao servidor cheguem até a máquina do cliente para mexer nelas.

Essa é uma vantagem bastante útil, pois o usuário não perde tempo e pode adiantar seus trabalhos diretamente pela internet. Em contrapartida, é preciso estar sempre conectado à rede e o limite de armazenamento

Alguns dos serviços de email mais populares e que usam o protocolo IMAP como base são o **Gmail**, do Google e o **Hotmail**, da Microsoft.

Num modelo de camadas, podemos estabelecer 3 conceitos, que estarão presentes em cada uma delas:

**Serviço:** o trabalho realizado pela camada propriamente.

**Interfaces:** comandos de comunicação entre camadas de uma mesma pilha.

**Protocolos:** regras de comunicação entre camadas correspondentes, em pilhas diferentes.

### **Modelo simplificado de 3 camadas:**

- **Acesso à rede** – Troca de dados entre o computador e a rede (acesso ao serviço disponibilizado pela rede) – O computador origem fornece à rede o endereço do computador de destino o que permite à rede encaminhar os pacotes de informação até ao nó de destino
- **Transporte** – Transferência de dados extremo-a-extremo (pretende-se em muitos casos que seja ordenada e fiável) – Independente da rede e da aplicação
- **Aplicação** – Exemplo: transferência de ficheiros, correio electrónico, acesso a computador remoto, etc.

### **Modelo OSI**

Em 1977 a ISO – *International Standardization Organization* criou o modelo de referência OSI – *Open Systems Interconnection*.

O objetivo da ISO foi estabelecer um modelo de camadas padronizado, ou seja, um modelo ao qual os desenvolvedores e outros pudessem se referir ao descrever seus protocolos ou outros componentes de software.

- **O Modelo de Referência de Sistemas Abertos** (Open Systems Interconnection Reference Model) define regras gerais de interacção entre sistemas abertos, isto é, sistemas que obedecem a normas universais de comunicação (por oposição a sistemas fechados ou proprietários)
- O Modelo OSI cria as bases para a especificação e aprovação de standards por organizações de normalização reconhecidas internacionalmente - embora os standards não façam parte do modelo

- **O Modelo OSI define princípios, conceitos e relações entre componentes** – é um modelo abstracto da descrição da comunicação entre sistemas (e não um modelo de implementação, i.e., não concretiza serviços, protocolos e tecnologias)

- **O Modelo OSI é geral e flexível** - embora definido no contexto das redes de computadores que se desenvolveram durante a década de 70, continuam a ser usados como modelo de descrição de redes e serviços que se desenvolveram desde então.

O Modelo OSI propõe uma organização funcional em sete camadas, de acordo com os seguintes princípios – As funções são decompostas e organizadas em camadas – Cada camada realiza um conjunto de funções relacionadas, suportadas num protocolo – Cada camada fornece serviços à camada superior escondendo-lhe os detalhes de implementação – Cada camada usa serviços da camada inferior – Mudanças internas numa camada não implicam mudanças nas outras camadas • O Modelo OSI não se pode reduzir a esta visão simplificada de sete camadas protocolares - pois inclui um conjunto extremamente rico de conceitos e princípios, nomeadamente – Princípios de estruturação em camadas – Modelo e Tipos de Serviço – Descrição das Funções a suportar pelos Protocolos das diferentes camadas – Princípios de Endereçamento



Figura 9: Modelo OSI

Neste ponto, é importante fazermos uma distinção entre:

**Modelo:** uma descrição abstrata (documental) que expressa “o **quê**” deve ocorrer em cada nível.

**Protocolo:** uma descrição abstrata (documental) que expressa “**como**” o que foi estabelecido no modelo será realizado.

**Implementação:** componentes de software ou hardware que irão “**fazer acontecer**” o que foi estabelecido pelo modelo/protocolo.

## 2.8 Segurança em Redes de Comunicação

Quando falamos em Segurança nas redes de computadores atualmente, fazemos uma grande referência à Internet, pois é nessa rede mundial onde os ataques aos nossos computadores ocorrem com maior frequência.

No campo de redes, a área de segurança de rede consiste na provisão e políticas adotadas pelo administrador de rede para prevenir e monitorar o acesso não autorizado, uso incorreto, modificação ou negação da rede de computadores e dos seus recursos associados.

Mas a vulnerabilidade segundo a ISO (International Standardization Organization - Organização Internacional para Padronização), no contexto da computação, é qualquer fraqueza que pode ser explorada para se violar um sistema ou as informações que nele contém.

Dessa forma, temos várias possíveis violações de segurança em um sistema, ou seja, temos várias ameaças, dentre as quais destacamos:

- Destruição de informação
- Modificação ou deturpação da informação
- Roubo, remoção ou perda de informação / recursos
- Interrupção de serviços

Por definição, temos ainda o ataque, que é a realização efetiva de uma ameaça de forma intencional. Como exemplos de ataques em computação, temos:

- Personificação (masquerade)
- DDos

- Replay
- Modificação
- Engenharia social
- Recusa ou impedimento de serviço

Mediante este ambiente de insegurança onde os dados estão inseridos e fluem nos sistemas e redes de computadores, é que muitas empresas adotam políticas de segurança, que são conjuntos de regras, leis e práticas de gestão visando à proteção. Podem ser implementadas com o uso de vários mecanismos, como por exemplo:

- Criptografia
- Assinatura digital
- Autenticação
- Controle de acesso
- Rótulos de segurança
- Detecção, registro e informe de eventos
- Enchimento de tráfego
- Controle de roteamento

Dessa forma, não sendo suficientes os mecanismos de segurança na rede como um todo, estabelecemos medidas de segurança nas comunicações também, como no correio eletrônico. Este (e-Mail) utiliza vários mecanismos para que nossos dados cheguem o mais possível seguro em seu destino. Faz uso de protocolos como SMTP (Simple Mail Transfer Protocol) que é considerado fraco, S/MIME (Secure Multipurpose Internet Mail Extensions) e PGP (Pretty Good Privacy) que é destinado à criptografia de e-mail pessoal.

O que está muito em uso são os Firewall's, dispositivos que funcionam como uma barreira de proteção contra invasores. Existem tanto na forma de software como de hardware, ou na combinação de ambos.

Como exemplo de bons firewall's domésticos e gratuitos, podemos citar:

- Comodo Firewall
- Zone Alarm
- Sygate Personal Firewall

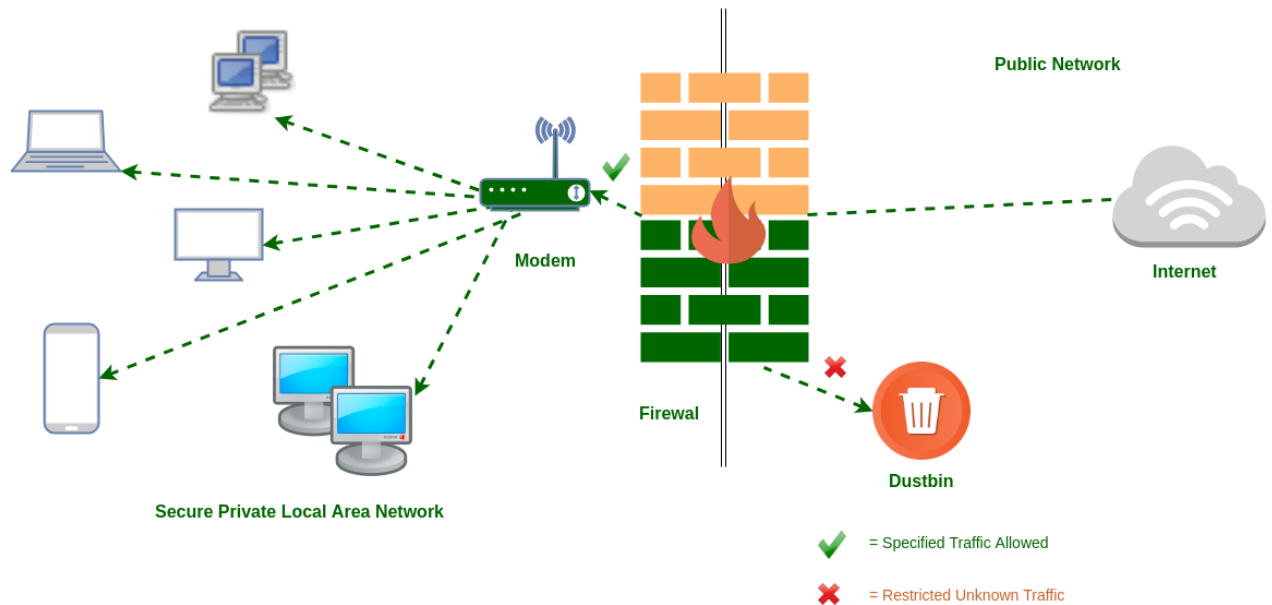


Figura 10: Medida de segurança

### 3. Caso Prático da Empresa/Organização

#### 3.1 Caracterização da entidade em estudo

**PowerSolution-** eletricidade, tecnologia e informática, Lda é uma start-up que surgiu em outubro de 2018, tem estado a dedicar ao desenvolvimento de projetos tecnológicos e comércio de produtos eletrotónicos; informáticos e consumíveis de laboratórios. Prover soluções tecnológicas e inovadores, que resolvam problemas da nossa realidade africana, promovendo a educação.

## **Missão**

Prover soluções tecnológicas e inovadores, que resolvam problemas da nossa realidade africana, promovendo a educação.

## **Visão**

Ser referência nacional e na região africana pela eficiência, eficácia e inovação nas nossas soluções tecnológicas.

## **Valor**

Inovação, eficácia, transparência, valorização humana e preocupação com satisfação dos clientes.



*Figura 11: logo da empresa*

### **3.2 Análise da situação atual**

Esta empresa possui alguns serviços tais como: Desenvolvimento de Sistemas Informáticos, Criação de logo, website e loja online, Manutenção e Reparação dos Equipamentos Informáticos e Electrónicos, Redes e Segurança Informática, Instalação e Manutenção de CFTV, Auditoria Energética, Dimensionamento do Sistema Solar Fotovoltaico, Vendas de Equipamentos Informáticos, Electrónicos e Eletrodomésticos.

### **Produtos inovadora dessa empresa:**

**Sisetema de Controlo de Acesso** que permite controlar acesso e assiduidade dos utilizadores da sua empresa, edifício e/ou instituição a partir do cartão de identificação do utilizador.

### **Sistema Eficiente da Recolha e Entrega**

Plataforma para otimização da rota - é uma solução tecnológica para otimizar a rota da recolha ou entrega de produtos.

**Sistema de Monitorização de Reservatório de Água** – “Agu Dja Seka?” é uma solução tecnológica que permite monitorizar água em tempo real a partir de uma aplicação mobile.

### **Pos parceiros dessa empresa**

Bic, nosi, univcv fct, fciftech, M&Tech technology and innovation

### **Contato dessa empresa**

**Endereço:** Av. Santiago nº28, Palmarejo, Praia, Santiago

**Website:** <https://powersolutioncv.com>

### **3.2.1 Projeto Lógico**

**Questionamento efectuado aos funcionarios dessa a empresa.**

**Quais os tipo de cabo usado nessa empresa?**

R: Cabo fibra optica que vai do provedor até o router , cabo directo para equipamento do mesmo tipo, cabo coaxial para camera de vigilância, cabo axial para tv, par-traçado tipo cat5 3 cat6.



**Quem é o vosso provedor de internet para essa empresa?**

R: CVMultimedia de Telecom, que já era cliente há muito tempo.

**Numeros de equipamento electrónico ligados na rede na empresa?**

R: No piso 0 tem um router que ligado ao fibra optica de cvmovel(Cvmultimedia) ao router(Technicolor TG784nV3) e 15 computadores ligado ao switch(ccpv), um servidor http, ftp e DHCP, e servidor linux(Cent7 que é open server e ipan, Cent8 que é mosquito) um impressora, no 5º piso dois computador e 2 impressora, 1 accessPoint e 1 switch no ultimo piso é usado computadores portateis e computador de mesa(4) e um impressora que ligado ao switch de marca HP.

**Quantas router existe nessa empresa?**

R: 1 router() no raíz do chão da empresa.

**Quantidade de Switch?**

R: Existe 3 switch (CCPv) , 3pp(Asus) e de marca HP

**Qual é o tipo de classe de rede usado nessa empresa?**

R: É usado a classe C.

**Quais é o ip de rede e subrede da empresa?**

R: *obs:Temos ip real mas por razão de segurança não vamos expor só vamos dar um ip idêntico, 192.168.7.0/24.*

**Quantas accessPoint tem nessa empresa?**

R: Nesta empresa tem dois(2) Access point Technicolor TG784nV3, TP-link

**Fala nos um pouco sobre segurança física e lógica dessa empresa?**

R: Sobre física existe sistema camera vigilancia 24h/24h, entrada com cartão com chip de reconhecimento, e sobre segurança logica sistema operativo windows 10 todos actualizados com activo sempre, monitoramento de rede.

**Porquê não tem firewall nessa empresa?**

R: Não temos firewall devido ao custo elevado.

**Quais são os protocolos usado nessa empresa?**

R: Nós usamos varios tipos de protocolos como: FTP, HTTP, SNMP, RDP, DHCP

**Fala nos sobre vossos servidor?**

R: Temos servidor window 7 2009 que local, temos srrvidor linux centOS open server para monitorização da rede e ipan para ferir Ip da rede, e CentOS8 Mosquitto e um servidor web externo no hostigator

**Fala nos sobre tipo cabo nessa empresa e porquê?**

R: Temos maioria o cabo cat5E por razão financeira e cat6 de fibra optica que liga provedor até o router.

### 3.2.2 Projeto Físico

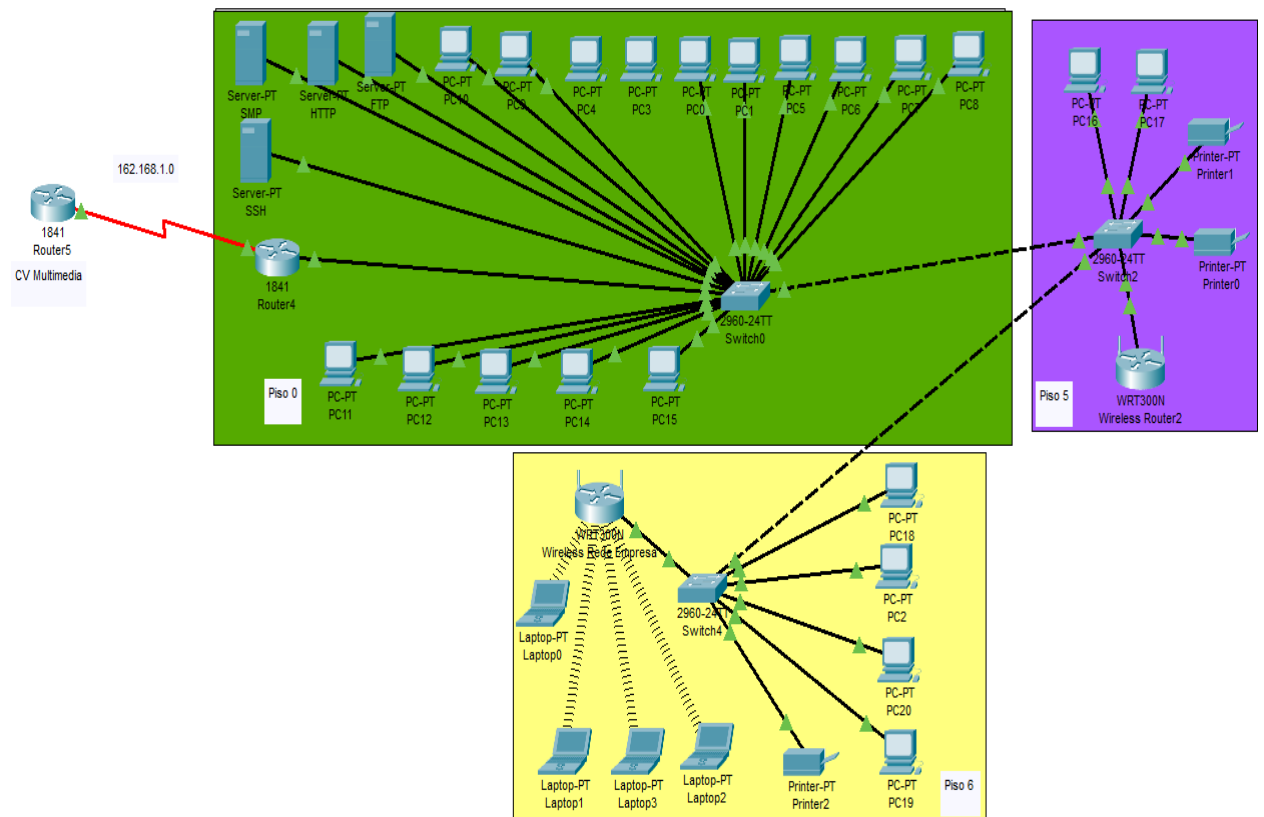


Figura 12: Rede da empresa

### 3.3 Proposta de melhorias

Reconhecido pela empresa para adquirir equipamento mais moderno como router usufrindo de mais recurso como segurança e desempenho

Levar a questão de segurança mais ao aserio como no questão de segurança lógico no aspecto de qualquer anomalia na rede possa dar resposta a tempo evitando maior ou pelo garantindo serviços minimos levando sempre encontra o backup dos ficheiro importante da empresa.

## **Conclusão**

Neste trabalho abordamos o boa parte do assunto da rede computadores no contexto teórico e prático que é da extrema importância numa instituição, empresa ou organização, portanto cumprimos todos os objetivos que tínhamos proposto perante o este trabalho que foi um trabalho muito importante para o nosso conhecimento.

Concluimos que esse trabalho foi feito através da organização e da partilha do conhecimento do grupo e boa vontade da empresa PowerSoltution, estando sempre de porta aberto para que possamos desenvolver e conhecer a rede de computadores na prática e a sua funcionalidade.

Agradecemos ao professor por ter dados essa oportunidade de criar elaborar esse trabalho porque é muito interessante e que por sua vez enriquecemos o nosso conhecimento.

## **Bibiografia**

Redes de Computadores, Andrew S. Tanenbaum 4ª edição, 2003.

PERCÍLIA, Eliene. "Segurança em Redes de Computadores

Analicia, Historia de rede <https://analicia-comdados.webnode.pt/historia-das-redes/>

Historia de Redes <https://ead.catolica.edu.br/blog/comunicacao-por-redes-de-computadores>

Wikipedia, Comunicacao de dados, [https://pt.wikipedia.org/wiki/Comunicao\\_de\\_dados](https://pt.wikipedia.org/wiki/Comunicao_de_dados)

Rede de Computadors, <http://masimoes.pro.br/redes-de-computadores/introducao/padroes-de-comunicacao.html>